Análisis de impacto en la implementación de DNSSEC en un servidor DNS Recursivo

Ernesto Sánchez[1], Daniel Arias Figueroa[1], Sergio Rocabado[1], Javier Díaz[2]

[1] Centro de Investigación en Informática Aplicada (C.I.D.I.A.). Universidad Nacional de Salta. Argentina.
[2] Universidad Nacional de la Plata. Provincia de Buenos Aires. Argentina
{esanchez, daaf, srocabad}@cidia.unsa.edu.ar

Abstract. Las extensiones de Seguridad para DNS (DNSSEC) proveen autenticación del origen e integridad de los datos intercambiados a través del protocolo DNS. Las mejoras que ofrece DNSSEC radican principalmente en el uso de una jerarquía de "firmas criptográficas" que permite proteger el flujo de información intercambiado entre Servidores Autoritativos, Servidores DNS Recursivos y Clientes DNS. En el presente trabajo se muestra la perspectiva desde un cliente DNS, es decir, como es el comportamiento y que costo en términos de tiempos de respuesta y carga de tráfico, de un servidor DNS Recursivo que debe realizar validaciones DNSSEC. Para poder exponer los aspectos antes citados, se comparó el comportamiento de un servidor DNS Recursivo tradicional, (sin características de seguridad), frente a un servidor DNS Recursivo DNSSEC

Keywords: DNSSEC, Extensiones de Seguridad para DNS, Estudio comparativo, Sistema de Nombres de Dominio, Universidad Nacional de Salta

1 Introducción

El despliegue a nivel mundial de las extensiones de seguridad para el Sistema de Nombres de Dominio (DNSSEC) ha alcanzado a la fecha el 88%, considerando que son 1405 los dominios de nivel superior en la zona raíz [1]. La implementación de tales extensiones ha sido relativamente lenta en términos de tiempo, si se tiene en cuenta que en el año 2010 se anunció el firmado de la zona raíz. Esto se debe principalmente a la naturaleza jerárquica del sistema DNS, donde cada eslabón de la cadena es administrado de forma independiente por entidades privadas, públicas, ISPs, etc. Otro aspecto crítico, que influye en la migración a DNSSEC, es la naturaleza del servicio de resolución de nombres, fundamental para el funcionamiento de Internet.

Otros aspectos no menos importantes, son los relacionados directamente con las nuevas características de DNSSEC, tales como, nuevos registros de recursos, criptografía de clave pública, proceso de validación de confianza entre zona padre y zona hijo, entre otros. Estos últimos influyen de manera directa en costos adicionales en términos de carga de tráfico y tiempos de respuesta en procesos de resolución de

nombres, donde se involucra a servidores DNS de diferentes características (De nivel superior, Autoritativos, Recursivos y Resolvers).

En el presente trabajo se muestra la perspectiva desde un cliente DNS, es decir, como es el comportamiento y que costo en términos de tiempos de respuesta y carga de tráfico, de un servidor DNS Recursivo que debe realizar validaciones DNSSEC. Para poder exponer los aspectos antes citados, se comparó el comportamiento de un servidor DNS Recursivo tradicional, (sin características de seguridad), frente a un servidor DNS Recursivo DNSSEC.

Las pruebas realizadas y resultados obtenidos, se obtuvieron en el marco de trabajo final de tesis de postgrado de la Universidad Nacional de la Plata. "Un estudio comparativo en extensiones de seguridad para el Sistema de Nombres de Dominio" (Expte 3300-2113/10-000)

2 Características de DNSSEC

En términos generales y según se describe en el RFC 4033: DNS Security Introduction and Requirements, las Extensiones de Seguridad para DNS (DNSSEC) proveen autenticación del origen e integridad de los datos intercambiados a través del protocolo DNS. Las mejoras que ofrece DNSSEC radican principalmente en el uso de una jerarquía de "firmas criptográficas" que permite proteger el flujo de información intercambiado entre Servidores Autoritativos, Servidores DNS Recursivos y Clientes DNS.

Para poder proveer los aspectos de seguridad anteriormente citados, DNSSEC hace uso de nuevos Registros de Recursos y una particular infraestructura de clave pública, basada en la construcción de una "cadena de confianza", necesaria para la validación de los datos en el proceso de consulta/respuesta DNS.

2.1 Nuevos Registros de Recursos

Los Registros de Recursos para DNSSEC son: [2].

- DNSKEY: Registro de Recurso habilitado para almacenar claves públicas, que posteriormente serán usadas por DNSSEC en procesos de autenticación.

- RRSIG: Contiene la firma para un conjunto de Registros de Recursos (RRset) con un nombre particular, clase y tipo. El registro RRSIG se genera en el proceso de firmado de una zona utilizando la clave privada y cuyo par (clave pública) es almacenada en el registro DNSKEY.

- NSEC: Permite validar la estructura de una zona y los Registros de Recurso que esta contiene.

- DS: Permite crear una cadena de confianza o de autoridad de una zona padre firmada, hacia una zona hija firmada. DS está relacionado con el Registro

DNSKEY, ya que contiene un resumen (hash o digesto) de la clave (KSK) almacenada en éste último.

2.2 Cadena de confianza

El proceso de construcción de una cadena confianza es fundamental para la implementación de DNSSEC en una jerarquía DNS, ya que sin ésta característica, cada Servidor Rescursivo configurado con DNSSEC, debería tener un punto de entrada seguro (SEP) por cada dominio seguro en Internet, lo que claramente haría imposible un despliegue a escala global de tales extensiones de seguridad. [9].

La siguiente ilustración permite observar los procesos involucrados en la creación de la cadena de confianza:

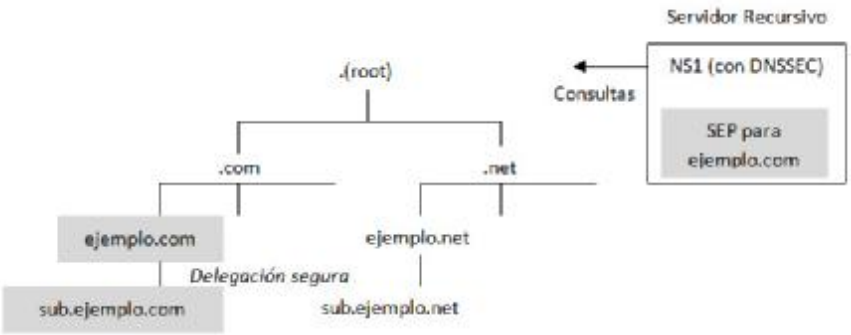

Fig. 1. Creación de cadena de confianza

Tanto el dominio ejemplo.com como sub.ejemplo.com se encuentran asegurados, es decir que para que pueda ocurrir una delegación segura es requisito previo haber asegurado la zona hija (sub.ejemplo.com). El punto de entrada seguro para ejemplo.com cubre las zonas seguras que son delegadas a partir de él, a través de una delegación segura creando una cadena de confianza provista por el uso del Registro de Recurso DS.

Una cadena de confianza puede ser construida tanto hacia arriba como hacia abajo en una jerarquía DNS, por lo que si el dominio de nivel superior .com fue asegurado, el dominio ejemplo.com puede unirse a la cadena.

Continuando con el ejemplo de la figura, el servidor NS1 (configurado con DNSSEC), podría ahora requerir un nuevo SEP para el dominio .com, y este único SEP cubriría ahora los dominios .com, ejemplo.com, así como sub.ejemplo.com.

Desde Julio 2010 la zona raíz se encuentra firmada y a la fecha, son 1257 los dominios de nivel superior que fueron firmados, de los cuales, 1245 tienen puntos de anclaje seguros publicados como registros DS en la zona antes mencionada [1]. Es importante resaltar que en Junio del año 2015, el dominio .ar, se encuentra asegurado y publicado en la zona raíz. [3].

2.3 Clave de Zona (ZSK) y Clave de Claves (KSK)

En los procesos de delegación y posterior validación de claves criptográficas de firmado, la siguiente clasificación de claves se hace necesaria a fin de facilitar las tareas operacionales llevadas a cabo por DNSSEC. Según se describe en el RFC 4641 [4], las claves usadas para el firmado de registros asociados a un dominio pueden ser de dos tipos, ZSK (Zone Signing Key) o KSK (Key Signing Key), donde la primera tiene por función la de proteger los Registros de Recursos individuales de una Zona dada, mientras que la KSK se encarga de proteger la ZSK. Operacionalmente se almacenan en un registro DNSKEY y se distinguen mediante el bit llamado SEP, presente en la porción RDATA del Registro de Recurso DNSKEY.

Algunas de las motivaciones para un uso separado de claves son: La KSK puede configurarse con longitudes de clave mayores, lo que la convierte en una clave de mayor fortaleza. Operacionalmente tiene poco impacto en consumo de recursos, ya que solo se usa para el firmado de una pequeña porción de datos de una zona dada. Por otro lado, dado que la KSK sólo se utiliza para firmar un conjunto de claves, ésta puede actualizarse con menos frecuencia que otros datos en la Zona y ser almacenada en una localización diferente de la ZSK.

3 Escenario de prueba utilizado

Según se expuso en 2.2, para poder garantizar la autenticidad e integridad de una respuesta DNS, en primera instancia se debe verificar la cadena de confianza desde el último eslabón de la cadena, hasta llegar al nodo raíz, es por esto que se configuró una jerarquía DNS, utilizando la herramienta de virtualización VMWare Player, según se muestra en la siguiente figura. Para la obtención de los datos se crearon dos instancias, la primera, basada en DNS tradicional y la segunda con extensiones de seguridad (DNSSEC)

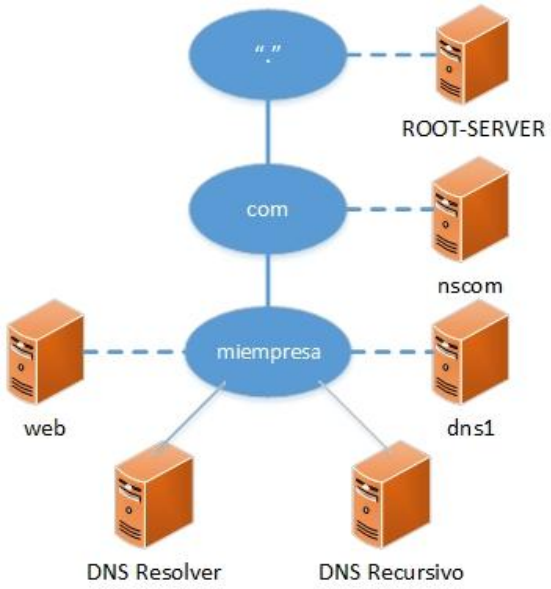

Fig. 2. Escenario de prueba

La siguiente tabla muestra detalles de la configuración utilizada, tales como direccionamiento IP y funcionalidad.

Tabla 1. Configuración escenario de prueba.

Nombre servidor	Dirección IP	Observaciones
ROOT-SERVER	10.0.0.254	Servidor DNS Raíz
nscom	10.0.0.253	Servidor TLD .com
dns1	10.0.0.2	Servidor Autoritativo miempresa.com
web	10.0.0.100	Servidor web miempresa.com
recursivo	10.0.0.11	Servidor Recursivo Cache
resolver	10.0.0.12	Cliente DNS

Todos los servidores están basados en Debian Linux con software DNS BIND versión 9.8.4

3.1 Generación de consultas DNS tradicional

Para el análisis de tráfico DNS se generaron consultas al dominio www.miempresa.com desde el servidor resolver, el cual retransmite las mismas al servidor recursivo. El primero ejecuta la herramienta Wireshark para la captura de los

paquetes de datos intercambiados. La siguiente tabla resume los datos que ilustran dos situaciones, donde la primera, el servidor recursivo, para responder a la solicitud del resolver, debe consultar al resto de los servidores, (Sin cache), mientras que en el segundo caso, responde a la consulta con los datos ya almacenados en cache, como consecuencia del primer caso.

Tabla 2. Datos obtenidos DNS tradicional.

DNS Tradicional	Consultas	Tiempo de rta	Bytes enviados	Bytes recibidos
Sin cache	4	0,0108 seg	341	514
Con cache	1	0,0039 seg	77	128

3.2 Configuración de escenario DNSSEC

Tomando como base el escenario presentado en la figura 2, se implementó DNSSEC en todos los servidores involucrados en la jerarquía DNS, es decir que, se configuró el servidor recursivo para validación DNSSEC, se firmaron zona raíz, zona .com y zona miempresa.com. El proceso se completó creando la cadena de confianza a partir de la publicación del registro DS desde zona hija a zona padre.

La implementación de DNSSEC para el escenario propuesto, se resume en los siguientes pasos:

- Generación de claves de firmado pública/privada ZSK y KSK.
- Publicación de claves pública ZSK y KSK en archivo de zona.
- Firmado de archivo de zona con clave privada ZSK.
- Publicación de archive DS en zona padre. Esto se realizó de zona .com a zona raíz y de zona miempresa.com a zona .com
- Refirmado de zona padre.
- Configuración de clave pública de validación inicial (KSK), para todos los servidores de la jerarquía, incluidos recursivo y resolver. Esta clave se obtuvo de lo generado en zona raíz (ROOT-SERVER).

Cabe resaltar que la configuración DNSSEC se realizó utilizando los comandos nativos provistos por BIND, siendo otras alternativas posibles, DNSSEC Tools, [6] y OpenDNSSEC, [7].

A modo de ejemplo se presenta la siguiente figura, la cual describe el recorrido de la cadena de confianza, la cual resulta de la configuración antes descripta.

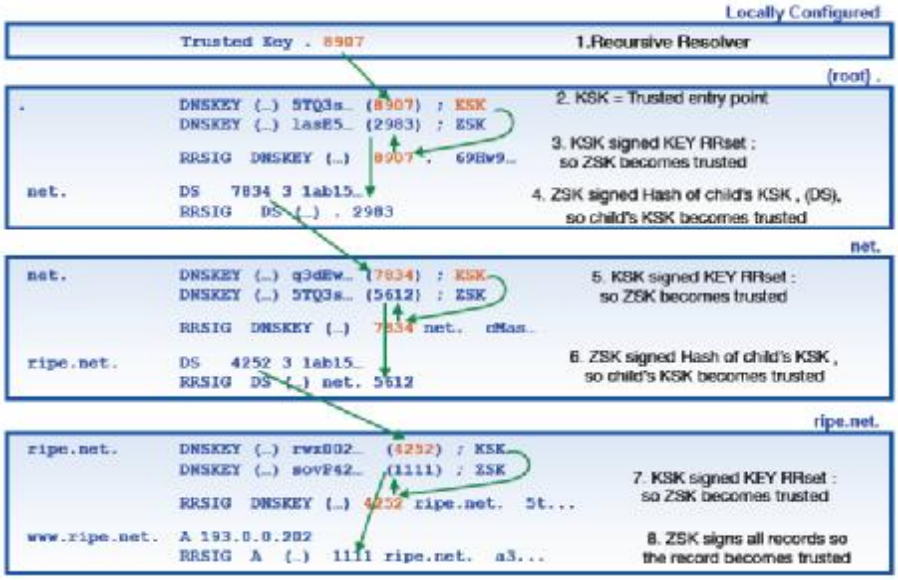

Fig. 3. Recorrido de cadena de confianza DNSSEC. [5]

3.3 Generación de consultas DNSSEC

Para la obtención de los datos en el proceso de consulta/respuesta, se usó la misma metodología del escenario DNS tradicional, es decir se generó una solicitud al dominio www.miempresa.com, en primera instancia sin cacheo y la segunda ya con datos almacenados en cache.

De los datos obtenidos de las pruebas, surge la primera observación importante, la misma se corresponde con el proceso de validación de la cadena de confianza, la cual se realiza en sentido contrario al proceso de consulta, la siguiente figura ilustra a modo de ejemplo dicha observación:

Fig. 4. Flujo de consulta y validación DNSSEC. [8]

Finalmente y con el propósito de realizar un estudio comparativo en cuanto a carga de tráfico y tiempos de respuesta, se registraron los siguientes datos:

DNSSEC	Consultas	Tiempo de rta	Bytes enviados	Bytes recibidos
Sin cache	9	0,0297 seg	727	6705
Con cache	1	0,0024 seg	77	128

Partiendo desde un estado en donde la cache local del servidor recursivo se encuentra vacía, se necesitan nueve consultas con un tiempo total para la resolución de la consulta de 0,0297 seg, con 727 bytes enviados y 6705 bytes recibidos. Lo que representa tres veces más de tiempo de respuesta, mientras que para el tráfico enviado el incremento es de 2,5 veces más y otras 10 veces más de carga de tráfico de salida, en comparación con el escenario DNS tradicional. En cuanto los datos de la consulta son almacenados en cache, la perfomance para la resolución mejora notablemente, demostrando que la funcionalidad de almacenamiento en cache es sumamente útil.

4 Conclusiones

Desde la perspectiva de un cliente DNS recursivo, se distinguen dos características fundamentales, la primera es que la funcionalidad de almacenamiento en cache, "absorbe" de manera eficiente, el impacto de la implementación de las extensiones de seguridad para DNS. Sin embargo, la puesta en marcha de tales aspectos de seguridad no se alcanza de manera inmediata, ya que requiere estar altamente familiarizado con el protocolo y el funcionamiento del mismo.

A la fecha, siguen surgiendo casos de implementación y documentación al respecto, lo que sumado a la adopción para el dominio .ar, permitirán continuar con las pruebas de perfomance sobre tráfico de consulta/respuesta sobre Internet.

Referencias

1. ICANN Research, TLD DNSSEC Report, http://stats.research.icann.org/dns/tld_report/
2. ARENDS, R., AUSTEIN, R., LARSON, M., MASSEY, D., AND ROSE, S. RFC 4034: Resource Records for the DNS Security Extensions, Marzo 2005.
3. NIC Ar. https://nic.ar/Enterate/Noticias/primera-ceremonia-de-dnssec-para-la-zona-ar
4. KOLKMAN, O, GIEBEN, R. RFC 4641: DNSSEC Operational Practices, Setiembre 2006.
5. RIPE Network Cordination Centre. DNSSEC Training Course. https://www.ripe.net/support/training/material/dnssec-training-course/DNSSEC-Slides-Single.pdf.
6. DNSSEC Tools Project. http://www.dnssec-tools.org/
7. Open DNSSEC Project. https://www.opendnssec.org/.
8. Sudan Network Operators Group. Hands on DNS and DNSSEC. http://www.sdnog.sd/images/SdNOG-2/DNSSEC/DNSSEC-course.pdf.
9. Ron Aitchison: Pro DNS and BIND. APRESS, New York (2011)